

II. CLAIM AMENDMENTS

1. (Currently Amended) A method for transmitting an encryption number in a communication system comprising: mobile terminals, and
at least a first access point and a second access point,
the method comprising:
defining a set of encryption keys,
selecting at each said access point from said set of encryption keys one to be used at a time for encrypting information to be transmitted between said access point and a mobile terminal,
transmitting from the access point, at intervals, data about the encryption key selected at the time,
setting up a data transmission connection between a mobile terminal and the first access point for the transmission of information, and
performing a handover, whereby a data transmission connection is set up between the second access point and the mobile terminal,
wherein in connection with the handover, information is transmitted over a broadcast control channel to the mobile terminal about the encryption key selected at the second access point, and
for the transmission of information about the encryption key such a broadcast control channel control field is selected which is not used as a general broadcast control channel control field.

2. (Previously Presented) The method according to claim 1, wherein each encryption key in said set of encryption keys is allocated an encryption number, and said encryption number is used as said data about the encryption key selected.

3. (Previously Presented) The method according to claim 1, in which information is transmitted in data frames, wherein the encryption key is changed in connection with each data frame.

4. (Previously Presented) The method according to claim 3, in which some of the data frames are used as common data frames for transmitting information from the second access point to more than one mobile terminal, wherein said data about the encryption key is transmitted in another data frame than said common data frame.

5. (Previously Presented) The method according to claim 1, wherein said set of encryption keys is stored in said access points and in the mobile terminal.

6. (Previously Presented) The method according to claim 1, wherein the mobile terminal informs said second access point about a need for handover, and said second access point transmits information about the encryption key selected at the second access point at the moment to the mobile terminal .

7. (Previously Presented) The method according to claim 1, wherein the mobile terminal informs said first access point about a need for handover, said first access point transmits information about the handover to said second access point, and said second access point transmits information about the encryption key selected at the second access point at the time to the mobile terminal.

8. (Previously Presented) The method according to claim 1, wherein the first access point executes a forced handover, in which the mobile terminal communicating with said first access point is transferred to communicate with said second access point, said

first access point transmits information about the handover to said second access point, and said second access point transmits information about the encryption key selected at the second access point at the time to the mobile terminal.

9. (Currently Amended) A mobile communication system comprising:

mobile terminals,

at least a first access point and a second access point;

a set of encryption keys being defined in the communication system;

the access point comprising a circuit means for selecting from said set of encryption keys one at a time to be used for encryption of information to be transmitted between said access point and a mobile terminal, and

a circuit means for transmitting information about the encryption key selected at the time at intervals from the access point;

the communication system also comprising:

a circuit means for setting up a data transmission connection between the mobile terminal and the first access point for the transmission of information, and

a circuit means for executing a handover and setting up a data transmission connection between the second access point and the mobile terminal,

wherein the mobile communication system also comprises a circuit means for transmitting over a broadcast control channel information about the encryption key selected at the second access point to the mobile terminal in connection with the handover, and

said means for transmitting are configured to select for the transmission of information about the encryption key such a broadcast control channel control field which is not used as a general broadcast control channel control field.

10.(Currently Amended) The mobile communication system according to claim 9, wherein it also comprises a circuit ~~means~~ for defining an encryption number for each encryption key in said set of encryption keys,

wherein said encryption number is arranged to be used as said information about the encryption key selected.

11.(Currently Amended) The mobile communication system according to claim 9, which comprises a circuit ~~means~~ for transmitting information in data frames, wherein the encryption key is arranged to be changed in connection with each data frame.

12.(Previously Presented) The mobile communication system according to claim 11, in which some of the data frames are arranged to be used as common data frames for transmitting information from one access point to more than one mobile terminal, wherein said data about the encryption key is arranged to be transmitted in another data frame than said common data frame.

13. (Previously Presented) The mobile communication system according to claim 9, wherein said set of encryption keys is stored at said access points and mobile terminal.

14. (Currently Amended) The mobile communication system according to claim 9, wherein the mobile terminal comprises a circuit ~~means~~ for informing said second access point about the need for a handover, and data is arranged to be transmitted from said second access point to the mobile terminal about the encryption key selected at the second access point at the time.

15. (Currently Amended) The mobile communication system according to claim 9, wherein the mobile terminal comprises a circuit means for informing said first access point about the need for handover.

16. (Currently Amended) The mobile communication system according to claim 9, wherein:

the first access point comprises a circuit means for performing a forced handover, the mobile terminal communicating with said first access point is arranged to be handed over to communicate with said second access point, and

a circuit means for transmitting information about the handover to said second access point, wherein information about the encryption key selected at the second access point at the time is arranged to be transmitted from said second access point to the mobile terminal.

17. (Previously Presented) The method according to claim 1, wherein said encryption keys are frame specific and are generated at both ends of said transmission connection.

18. (Previously Presented) The mobile communication system according to claim 9, wherein said encryption keys are frame specific and are generated at both ends of said transmission connection.

19. (Currently Amended) A network element comprising:

a circuit means for selecting from a set of encryption keys one at a time to be used for encryption of information to be transmitted between said access point and a mobile terminal, and

a circuit means—for transmitting information about the encryption key selected at the time at intervals from the access point;

wherein said circuit means—for transmitting isare configured to transmit over a broadcast control channel information about the selected encryption key to the mobile terminal in connection with a handover, and

said circuit means—for transmitting isare configured to select for the transmission of information about the encryption key such a broadcast control channel control field which is not used as a general broadcast control channel control field.

20. (Previously Presented) A network element according to claim 19 wherein it is an access point of a communication network.

21. (Currently Amended) A network element comprising:

a selector for selecting from a set of encryption keys one at a time to be used for encryption of information to be transmitted between said access point and a mobile terminal, and

a transmitter for transmitting information about the encryption key selected at the time at intervals from the access point;

wherein said transmitter is configured to:

transmit over a broadcast control channel information about the selected encryption key to the mobile terminal in connection with a handover, and

select for the transmission of information about the encryption key such a broadcast control channel control field which is not used as a general broadcast control channel control field.